ONLINEDURCHSUCHUNG

CCC enttarnt Bundestrojaner

Die viel debattierte Onlinedurchsuchung funktioniert: Der Chaos Computer Club hat die Spähsoftware untersucht. Sie kann und tut viel mehr, als die Verfassung erlaubt.

VON Kai Biermann | 08. Oktober 2011 - 21:30 Uhr


```
; =============== S U B R O U T I N E
=======================================

0zapftis_file_execute proc near        ;
CODE XREF:
_0zapftis_download_store_EXE+19Fp

var_D1= byte ptr -0D1h
hProcess= dword ptr -0D0h
var_CC= byte ptr -0CCh
lpProcName= dword ptr -0C8h
Msg    = byte ptr -0BCh
var_B8= dword ptr -0B8h
ExitCode= byte ptr -0A0h
var_9C= dword ptr -9Ch
var_98= dword ptr -98h
var_94= dword ptr -94h
var_90= dword ptr -90h
var_8C= dword ptr -8Ch
var_80= dword ptr -80h
var_64= dword ptr -64h
var_60= dword ptr -60h
var_50= dword ptr -50h
var_40= dword ptr -40h
```

```
          rep stosd
          mov     al, [esp+0E4h+arg_C]
          mov     [esp+0E4h+var_50], 44h
          mov     cl, al
          mov     [esp+0E4h+var_24], 1
          neg     cl
          sbb     ecx, ecx
          and     ecx, 0FFFFFFFBh
          add     ecx, 5
          test    al, al
          mov     [esp+0E4h+var_20], cx
          jz      short loc_10003C02

          mov     eax, 1388h
          mov     [esp+0E4h+var_24], 85h
          mov     [esp+0E4h+var_40], eax
          mov     [esp+0E4h+var_3C], eax

loc_10003C02:
; CODE XREF: _0zapftis_file_execute+62j
          mov     edx, [esp+0E4h+arg_14]
          mov     ecx, 0Fh
          xor     eax, eax
          lea     edi, [esp+0E4h+var_9C]
```

Ausschnitt aus dem Code der staatlichen Spähsoftware. Dieser Teil ermöglicht das heimliche Nachladen von Programmen auf den Rechner.

Der Chaos Computer Club hat mehrere Exemplare des sogenannten Bundestrojaners gefunden. Spätestens seit 2008 ist bekannt , dass die Polizei solche Spähsoftware nutzt, um unbemerkt in Rechner von Verdächtigen einzudringen. Bislang hat sie aber kein normaler Mensch zu Gesicht bekommen. Eine Version dieser intern "Remote Forensic Software" genannten Wanze haben Experten des CCC nun gründlich analysiert (hier der Bericht als PDF).

Ihr Urteil: Die viel diskutierte Onlinedurchsuchung funktioniert. Ermittler von Landeskriminalämtern, vom Zoll oder dem Bundeskriminalamt können auf fremde Computer zugreifen und sich von ihnen beliebige Informationen holen – und sie tun es auch, obwohl sie das gar nicht dürfen.

Denn im Jahr 2008 hatte das Bundesverfassungsgericht diese Art der Überwachung stark eingeschränkt und den Ermittlern enge Grenzen gesetzt. Polizeibehörden und Politiker von Union und SPD hatten zuvor gefordert, es müsse möglich sein, via Internet die Computer von Verdächtigen zu untersuchen und auf deren Festplatten gefundene Indizien zu sichern. Kritiker sahen darin eine Verletzung diverser in der Verfassung garantierter Rechte.

Angesichts der nun entdeckten Spähsoftware entsteht der Eindruck, dass sich die Behörden nicht an die vom Verfassungsgericht gesetzten Beschränkungen halten und sogar bewusst dagegen verstoßen.

Was hat der CCC entdeckt?

Nach Aussagen mehrerer Clubmitglieder hat der CCC auf dem Rechner einer Person, gegen die ein Ermittlungsverfahren lief, eine *Skype Capture Unit* gefunden. Das ist ein Programm, das entwickelt wurde, um die normalerweise verschlüsselten Chats und Gespräche via Skype abhören zu können.

Das allein wäre rechtlich erlaubt. Denn das Bundesverfassungsgericht hatte in seinem Urteil zwar die Onlinedurchsuchung, also das komplette Kopieren eines fremden Rechners stark beschränkt, nicht aber das Abhören von Kommunikation. Das wird durch die Telekommunikations-Überwachungsverordnung (TKÜV) geregelt und als "Quellen-TKÜ" bezeichnet, da es eine Kommunikation an der Quelle, also auf dem Rechner des Betroffenen, belauscht. Die gefundene Software allerdings konnte mehr, als erlaubt ist – und das wurde auch ausgenutzt.

Wie kommt die Spähsoftware auf den Rechner?

Das ist grundsätzlich auf zwei Wegen möglich. Entweder gelangen Polizisten kurz an das Gerät, um das Programm zu installieren, beispielsweise, indem sie in die Wohnung einbrechen, in dem es steht. Oder sie spielen das Programm über das Internet auf, indem sie einen sogenannten Trojaner nutzen – eine Software, die eine Schwäche des Zielsystems oder des Nutzers verwendet, um sich einzunisten und die dann das eigentliche Spionage-Programm installiert.

Was macht die gefundene Software?

In erster Linie belauscht sie Skype-Gespräche und schickt deren Inhalt an eine Behörde. Bei jedem Start des Computers fährt das Programm hoch und versucht, sich mit einem bestimmten Server im Internet zu verbinden. Werden über Skype Daten ausgetauscht, schneidet das Programm sie mit und schickt sie an diesen Server. Der stand in diesem Fall übrigens in den USA. Offensichtlich wollten die Ermittler damit den Zielort des Datenversands verschleiern.

Doch die gefundene Software kann noch einiges mehr. Sie macht auch alle paar Minuten ein Bildschirmfoto des entsprechenden Rechners und schickt diese Bilder ebenfalls an den von der Behörde gemieteten Server.

Das aber ist keine Quellen-TKÜ mehr. Es nicht mal mehr eine TKÜ, also eine Überwachung der Telekommunikation. Denn was jemand auf seinem Bildschirm sieht oder was er dort eintippt, sei es in ein Word-Dokument oder in ein Browser-Fenster, gilt nicht als Kommunikation. Solche Daten gelten als privat. Das Urteil

des Bundesverfassungsgerichts war in diesem Punkt sehr klar . Die Richter leiteten daraus sogar ein neues Grundrecht ab, das Recht auf die Integrität und Vertraulichkeit informationstechnischer Systeme, auch IT-Grundrecht genannt. Die vom CCC untersuchte Spähsoftware verstieß wochenlang alle paar Minuten gegen dieses Grundrecht.

Was kann die gefundene Software noch?

Daneben besitzt das Programm noch weitere Funktionen, die alle gegen das IT-Grundrecht verstoßen und keine Quellen-TKÜ darstellen. So befinden sich in dem Spähprogramm Teile eines Keyloggers . Der merkt sich jede Tastatureingabe und sendet sie an die Behörde. So können nachträglich auch Passwörter in Erfahrung gebracht werden – jede Verschlüsselung wird sinnlos.

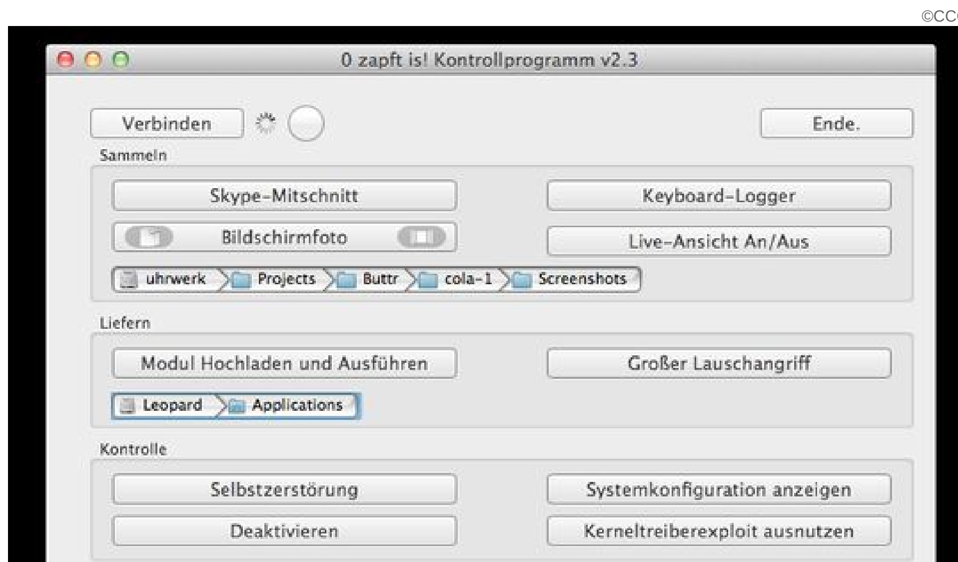
An das Programm können außerdem neue Programmteile angedockt werden, die dann beispielsweise eine etwaige Kamera des Rechners und/oder sein Mikrofon steuern. Damit ist es möglich, eine unbemerkte Überwachung des Raumes vorzunehmen, in dem der Rechner steht. Das aber ist ein Großer Lauschangriff , der nur bei "besonders schweren Straftaten" erlaubt ist. Mit einer Quellen-TKÜ, wie sie in diesem Einzelfall der Richter genehmigt hatte, hat das nichts mehr zu tun.

Das Programm könnte außerdem eine komplette Onlinedurchsuchung durchführen, also die Festplatte des Zielrechners nach Informationen durchstöbern oder gleich die ganze Platte kopieren und die Kopie an die Behörde schicken. Auch das ist keine Quellen-TKÜ und unterliegt strengen Beschränkungen.

Die Computerforensiker des CCC konnten nicht feststellen, ob diese Funktionen von der Polizei auch tatsächlich eingesetzt wurden. Sie wissen nur, dass sie vorhanden sind oder nachträglich über das Internet installiert werden können – was ganz nebenbei das Bundesinnenministerium der Lüge überführt. Das Ministerium hatte 2007 der SPD-Fraktion im Bundestag schriftlich versichert , man werde die Software so programmieren, "dass sie keine Daten frei im Zielsystem platzieren kann". Der Trojaner aber hat eindeutig die Fähigkeit, sich Daten aus dem Internet zu holen und auf die Festplatte des Zielrechners zu schreiben.

Wie wurde das Spähprogramm überhaupt entdeckt?

Die Beamten haben offensichtlich gepfuscht. Das Programm enthält theoretisch eine Art Selbstmordfunktion: Auf ein von außen kommendes Kommando hin sollte es sich selbst löschen. Constanze Kurz, Informatikerin und eine der Sprecherinnen des CCC, sagt dazu: "Das Programm wurde nur in den Papierkorb geschoben und nicht überschrieben." Es war also nicht unwiderruflich gelöscht. Dem Chaos Computer Club seien mehrere Festplatten anonym zugeschickt worden und die Forensiker hätten keine Probleme gehabt, es zu rekonstruieren. Und nicht nur das: Die CCC-Experten konnten die Software auch wieder zum Laufen bringen. Nun können sie das Programm nach Belieben steuern .



Vom Chaos Computer Club (CCC) entwickeltes Programm zur Steuerung des Bundestrojaners.

Das ist insofern peinlich, weil das Innenministerium vor vier Jahren in einer zweiten schriftlichen Antwort, dieses Mal auf Anfragen des Bundesjustizministeriums , erklärt hatte, die Spähprogramme würden "einen wirksamen Schutz gegen Missbrauch" enthalten. Zitat: "Speziell wird sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den vom Bundeskriminalamt verwendeten zurückzumelden, und dass die Software weder von außen erkannt noch angesprochen werden kann."

Frank Rieger, ebenfalls Sprecher beim CCC und Experte für Verschlüsselungsverfahren, kann darüber nur lachen. "Das Ding hat keine Sicherheitsmaßnahmen", sagt er. Lediglich die abgelauschten Daten seien beim Verschicken verschlüsselt, die Steuerbefehle an das Programm jedoch kämen im Klartext an.

Der Trojaner stelle für den Überwachten zudem eine erhebliche Gefahr dar, sagt Rieger. "Er öffnet den Rechner komplett. Wer sich dann damit in einem ungesicherten Netz bewegt, ist schutzlos." Oder, wie CCC-Mitglied Felix von Leitner bloggt : "Wenn dieser Trojaner auf einem Rechner installiert ist, steht der danach für jeden offen wie ein Scheunentor."

Dazu ein Zitat des Innenministeriums von 2007: "Es soll bei der Onlinedurchsuchung eine selbst entwickelte Software eingesetzt werden, die auch unter den Gesichtspunkten möglicher Risiken für Betroffene und unbeteiligte Dritte entsprechend hinreichend geprüft sein wird."

Wird die Spähsoftware von Virenscannern erkannt?

Nein, bislang nicht. Hersteller von Antivirenprogrammen haben jedoch schon vor Jahren angekündigt, dass sie ihre Produkte gegen jedes Schadprogramm wappnen, auch wenn es von einer Behörde programmiert wurde. Da der Chaos Computer Club den kompletten

Binärcode des Spähprogramms veröffentlichen will, ist anzunehmen, dass bald alle großen Antivirenhersteller diesen in ihre Filter aufnehmen. Künftig also würde ein Behördenspäher dieser Bauart herausgefischt.

Kann man sich gegen eine solche Infiltrierung schützen?

Nur mühsam. Es gibt einen Weg, so ein Spähprogramm zu enttarnen. Dazu muss ein Nutzer den Datenverkehr seines Rechners überwachen. Sendet dieser beispielsweise in regelmäßigen Abständen große Bilddateien an einen unbekannten Server im Netz, ist möglicherweise etwas faul.

Ein besserer Schutz wäre klarere Gesetze. Der CCC fordert denn auch zwei Dinge: Erstens müsse endlich sauber geregelt werden, welche Ermittlungsverfahren wann zulässig sind und welche nicht. Es gebe immer noch zu viele Grauzonen, sagt Rieger. Und zweitens müsse verboten werden, illegal erlangte Beweise verwerten zu dürfen. Denn bislang darf die Polizei zum Beispiel die mit Hilfe des Trojaners erstellten Screenshots für eine Anklage nutzen – auch wenn sie diese Dateien eigentlich gar nicht haben dürfte. Und grundsätzlich findet der Club, dass "die heimliche Infiltration von informationstechnischen Systemen durch staatliche Behörden" beendet werden müsse.

Denn es stellt sich die Frage, wie der Einsatz eigentlich kontrolliert wird. Mit entsprechenden Strafsachen beauftragte Anwälte schätzen, dass in den vergangenen Jahren 80 bis 100 solcher Programme heimlich bei Verdächtigen eingeschleust wurden. Welche davon nur genau das erspähten, was sie durften und welche viel mehr – das wissen nur die Ermittler.

ADRESSE: http://www.zeit.de/digital/datenschutz/2011-10/ccc-bundestrojaner-onlinedurchsuchung